

# Depolarizing-channel parameter estimation using noisy initial states

David Collins\* and Jaimie Stephens

*Department of Physical and Environmental Sciences, Colorado Mesa University, Grand Junction, Colorado 81501, USA*

(Received 19 June 2015; published 25 September 2015)

We consider estimating the parameter associated with the qubit depolarizing channel when the available initial states that might be employed are mixed. We use quantum Fisher information as a measure of the accuracy of estimation to compare protocols which use collections of qubits in product states to one in which the qubits are in a correlated state. We show that, for certain parameter values and initial states, the correlated-state protocol can yield a greater accuracy per channel invocation than the product-state protocols. We show that, for some parameters and initial states, using more than two qubits and channel invocations is advantageous. These results stand in contrast to the known optimal case that uses pure initial states and a single channel invocation on a pair of entangled qubits.

DOI: [10.1103/PhysRevA.92.032324](https://doi.org/10.1103/PhysRevA.92.032324)

PACS number(s): 03.67.-a, 03.65.Ta, 03.65.Ud

## I. INTRODUCTION

Quantum parameter estimation, originally motivated by optical metrology [1–3], considers how to estimate parameters associated with the evolution of quantum systems by physical means. A theory of quantum estimation, derived from the laws of quantum physics and statistics, has been developed and applied to various evolution processes yielding important results for various metrology situations [1,2,4–11].

We consider the single-qubit depolarizing channel, which maps a qubit, initially in the state  $\hat{\rho}$ , via

$$\hat{\rho} \mapsto \hat{\rho}_t(\lambda) := \frac{1-\lambda}{2} \text{Tr}[\hat{\rho}] \hat{I} + \lambda \hat{\rho}, \quad (1)$$

where  $0 \leq \lambda \leq 1$ . The aim of a physical estimation protocol would be to determine  $\lambda$  as accurately as possible by subjecting a collection of qubits to this evolution.

The depolarizing channel is interesting for various reasons. First, depolarization is a standard model of certain noise processes and is of general interest for quantum information processing [10,12–15]. Specific examples appear in nuclear magnetic resonance (NMR) [16,17] and optical quantum information processing [18–20].

Second, quantum parameter estimation reveals fundamental and quantifiable differences with classical approaches when manifestly quantum resources such as entanglement are used. For example, in the estimation of the phase associated with a unitary parameter, classical approaches yield an uncertainty that scales as  $O(1/\sqrt{n})$ , where  $n$  is the number of times the channel is invoked, whereas using entangled states can result in a lower uncertainty that scales as  $O(1/n)$ , thus pointing to a measurable gain provided by entanglement [8,21,22].

Depolarizing-channel parameter estimation has been investigated previously in the context of finding optimal estimation protocols [23–26] where any possible initial state is assumed to be available. It emerges that the optimal estimation protocol requires qubit pairs, each initially in an entangled pure state, and that states displaying entanglement or correlations among

more than two qubits will not give any advantages to estimation accuracy [25].

We consider various estimation protocols for the constrained situation when the available initial state of each qubit is mixed. This situation arises in room-temperature solution-state NMR, where the initial state for any nuclear spin is highly mixed [14]. We ask whether, for mixed-initial-state situations, protocols involving correlated states can yield gains in estimation accuracy compared to protocols that use product states and whether increasing the number of correlated qubits beyond two is advantageous. While we will consider these questions for situations involving initial states with all possible ranges of mixedness, we will focus on the special case where the initial state of each qubit is highly mixed. Our approach is motivated by similar work for other types of channels where gains were found when using correlated states [27,28] and is also inspired by various other approaches to investigating parameter estimation with mixed initial states [29–33].

This article is organized as follows. Section II offers a review of quantum estimation theory. Section III applies this to the simplest depolarizing-channel-parameter channel-estimation protocol, establishes a benchmark against which other schemes are to be compared, and reviews existing results for parameter estimation using pure initial states. Section IV considers mixed-initial-state estimation protocols where there are never any correlations between qubits. Section V, which contains the key general results of our article, considers an estimation protocol that employs correlated states. Section VI applies these to the special case where the available initial states are highly mixed. Finally, Sec. VII briefly discusses the roles of entanglement and quantum discord in the protocol that uses correlated states.

## II. QUANTUM PARAMETER ESTIMATION

Physical parameter estimation requires that suitably prepared quantum systems be subjected to the operation  $\hat{\Gamma}(\lambda)$ , which is dependent on a real parameter  $\lambda$  that is to be estimated. The generic scheme for doing this, illustrated in Fig. 1, assumes that  $m$  copies of the operation, or channel, are available. These may be invoked on one or more of  $n$  systems with invocations surrounded by a series of parameter-independent unitary transformations. Each quantum system is prepared in a known

\* Author to whom correspondence should be addressed.  
dacollin@coloradomesa.edu

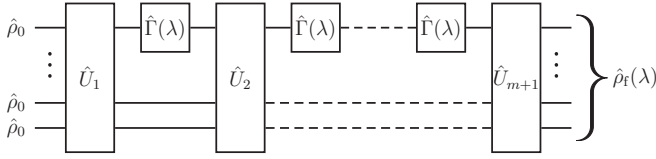


FIG. 1. Quantum estimation procedure using  $n$  quantum systems, each represented by a horizontal line. This procedure uses  $m$  invocations of the operation  $\hat{F}(\lambda)$  and parameter-independent unitary transformations  $\hat{U}_1, \dots, \hat{U}_{m+1}$ . The initial state of each quantum system is  $\hat{\rho}_0$ , and the premeasurement state of the collection of systems is  $\hat{\rho}_f(\lambda)$ . Measurements on individual systems follow  $\hat{U}_{m+1}$ .

initial state  $\hat{\rho}_0$ . After the final unitary, a measurement is chosen and performed on each system, and the measurement outcomes are recorded. The final premeasurement state  $\hat{\rho}_f(\lambda)$  may depend on the parameter and thus so will the probabilities with which the measurement outcomes occur. Thus information about  $\lambda$  might be inferred from the measurement outcomes by classical data processing, thus yielding an estimate for the parameter.

The fact that measurement outcomes in quantum physics are usually statistically distributed implies that different runs of the same estimation procedure will yield estimates that fluctuate about a mean value. The aim of quantum parameter estimation is to tailor the process by choosing the initial state  $\hat{\rho}_0$ , the parameter independent unitaries  $\hat{U}_1, \dots, \hat{U}_{m+1}$ , and the final measurements so that the estimates will display minimal fluctuations about the actual parameter value.

The accuracy of the estimation is quantified via these statistical fluctuations as follows. Given a set of measurement outcomes, one on each qubit and denoted  $\{x_1, \dots, x_n\}$ , an estimate for the parameter  $\tilde{\lambda}$  is attained via  $\tilde{\lambda} = \lambda_{\text{est}}(x_1, \dots, x_n)$ , where  $\lambda_{\text{est}}$  is an estimator function. Fluctuations in these measurement outcomes from one run of the estimation procedure to another generate fluctuations in  $\tilde{\lambda}$ . The extent to which this occurs depends on the construction of the estimator function. Key requirements for an estimation protocol will be that the estimator is unbiased, i.e.,  $\langle \tilde{\lambda} \rangle = \lambda$ , and that it minimizes the variance,

$$\text{var}(\tilde{\lambda}) := \langle (\tilde{\lambda} - \langle \tilde{\lambda} \rangle)^2 \rangle, \quad (2)$$

where the angle brackets indicate the mean over all possible measurement outcomes. The variance will depend on the choice of estimator. However, a key result [9,34,35] is that the variance on any estimator is bounded from below via the Cramér-Rao bound

$$\text{var}(\tilde{\lambda}) \geq \frac{1}{F(\lambda)}, \quad (3)$$

where

$$F(\lambda) := \int \left[ \frac{\partial \ln p(x_1, \dots, x_n | \lambda)}{\partial \lambda} \right]^2 dx_1 \dots dx_n \quad (4)$$

is the (classical) Fisher information associated with the probability distribution for the measurement outcomes  $p(x_1, \dots, x_n | \lambda)$ . This is independent of the choice of estimator. Quite generally, there is always an estimator [34], which asymptotically saturates the bound of Eq. (3). Thus in classical parameter estimation the Fisher information quantifies the

accuracy of any possible estimate; the larger  $F(\lambda)$  is, the better the estimate is.

In classical estimation, it is easily shown [35] that if the same estimation trial is repeated  $m$  times independently, the Fisher information becomes  $mF(\lambda)$ , where  $F(\lambda)$  is the Fisher information for a single trial. Thus the Cramér-Rao bound implies a reduction in the variance by a factor of  $m$ , yielding the typical classical reduction in uncertainty of the estimate by a factor of  $\sqrt{m}$ .

In quantum evolution processes the probability distribution for the measurement outcomes depends on the type of measurement. Thus, given many possible choices of measurement, there will be many possible values for the classical Fisher information for the same evolution process. Quantum estimation aims for a measurement which results in the largest classical Fisher information. This is constrained and simplified by the *quantum Cramér-Rao bound*, which states that for any measurement the resulting classical Fisher information satisfies

$$F(\lambda) \leq H(\lambda), \quad (5)$$

where  $H(\lambda)$  is the quantum Fisher information and is independent of the choice of measurement [5,9,35,36]. The quantum Fisher information depends only on  $\hat{\rho}_f(\lambda)$  and is calculated via [9]

$$H(\lambda) = \text{Tr}[\hat{\rho}_f(\lambda) \hat{L}^2(\lambda)], \quad (6)$$

where the symmetric logarithmic derivative (SLD), or score operator,  $\hat{L}(\lambda)$  is defined implicitly via

$$\frac{\partial \hat{\rho}_f(\lambda)}{\partial \lambda} = \frac{1}{2} [\hat{L}(\lambda) \hat{\rho}_f(\lambda) + \hat{\rho}_f(\lambda) \hat{L}(\lambda)]. \quad (7)$$

In general the SLD is not immediately apparent from  $\hat{\rho}_f(\lambda)$ ; sometimes it can be computed using relatively simple algebra [28]. However, the SLD and quantum Fisher information can always be computed whenever an eigenvalue and eigenstate decomposition for  $\hat{\rho}_f(\lambda)$  can be found. Specifically, if  $\hat{\rho}_f(\lambda) = \sum_j p_j |\phi_j\rangle \langle \phi_j|$ , then [9]

$$H = \sum_j p_j \left( \frac{1}{p_j} \frac{\partial p_j}{\partial \lambda} \right)^2 + 2 \sum_{j,k} \frac{(p_j - p_k)^2}{p_j + p_k} \left| \langle \phi_j | \frac{\partial |\phi_k\rangle}{\partial \lambda} \right|^2. \quad (8)$$

Quite generally, there exists a measurement procedure which asymptotically attains the quantum Cramér-Rao bound [37]. Thus the quantum Fisher information quantifies the accuracy of the quantum estimation process. The main task in quantum parameter estimation is to provide a protocol giving a final premeasurement state  $\hat{\rho}_f(\lambda)$  with the maximum quantum Fisher information; this approach has been widely adopted elsewhere [5,7–9,11,22,23,25–28,32,35,38–42].

Before continuing, we remark that a useful computational alternative to Eq. (6) is [28]

$$H(\lambda) = \text{Tr} \left[ \frac{\partial \hat{\rho}_f(\lambda)}{\partial \lambda} \hat{L}(\lambda) \right]. \quad (9)$$

The quantum Fisher information will depend on the resources, such as the numbers of qubits, channel invocations, single-qubit unitaries, or entangling unitaries that are used, and

various competing estimation protocols can only be compared in terms of their resource use. In this article we take a common approach, which regards the number of channel invocations  $m$  in the circuit of Fig. 1 as the only important resource cost [9,11,21,22,43]. In this context, the goal of any quantum estimation protocol is to produce a final state with the maximum quantum Fisher information per channel invocation.

The initial state for the entire system can be assumed to be a product of states for the individual systems. If necessary, any of  $\hat{U}_1, \dots, \hat{U}_{m+1}$  can be used to generate entangled or otherwise correlated states as the procedure unfolds. We can then consider two broad classes of estimation schemes. In the first the unitaries  $\hat{U}_1, \dots, \hat{U}_{m+1}$  never produce any correlation between the individual systems, and the entire system evolves through a series of product states. Various classical approaches to estimation, including repetition and averaging, fall into this realm. In the second, some of the unitaries  $\hat{U}_1, \dots, \hat{U}_{m+1}$  produce states where there is some form of quantum correlation, such as entanglement, between the individual systems. Frequently, quantum estimation aims to show that using such correlated states results in a parameter estimate with greater quantum Fisher information per channel invocation [8,23,27,28,39] than is possible with noncorrelated states; indirectly, this indicates the utility of quantum resources for information processing.

#### A. Initial-state considerations

Within the framework of Fig. 1, the typical task is to find the initial state  $\hat{\rho}_0$  and the unitaries  $\hat{U}_1, \dots, \hat{U}_{m+1}$  that produce a final state  $\hat{\rho}_f(\lambda)$  that yields the maximum quantum Fisher information per channel invocation. The convexity of the quantum Fisher information guarantees that this will be attained by using a pure initial state [23,40], and most investigations of depolarizing-channel parameter estimation have considered this case [23–26]. However, it may be the case that the available initial states are not pure. Our aim is to consider various estimation protocols when the available initial states are limited to those that are mixed.

The general initial state of a single qubit is

$$\hat{\rho}_0 = \frac{1}{2} (\hat{I} + \mathbf{r} \cdot \hat{\boldsymbol{\sigma}}), \quad (10)$$

where  $\mathbf{r} \cdot \hat{\boldsymbol{\sigma}} = r_x \hat{\sigma}_x + r_y \hat{\sigma}_y + r_z \hat{\sigma}_z$  and  $r_x, r_y, r_z$  are the components of a three-dimensional real vector  $\mathbf{r}$ . The magnitude of this vector  $r := \sqrt{r_x^2 + r_y^2 + r_z^2}$  is called the *polarization* or *purity* of the state and it satisfies  $0 \leq r \leq 1$ . When  $r = 1$ , the state is pure, and as  $r$ , which we use to quantify the mixedness or purity of the state, decreases, the state becomes more mixed.

Thus the principal issue of such mixed-state quantum estimation is, Given that the available qubits have initial states each with polarization  $r$ , how do the accuracies, quantified by the quantum Fisher information, of various parameter-estimation protocols compare? Note that, in this approach, the orientation of the polarization vector  $\mathbf{r}$  is irrelevant, as this can be modified at no cost with a single-qubit unitary without changing the polarization  $r$ .

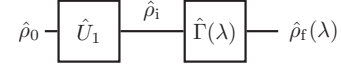


FIG. 2. SQSC protocol. The qubit is initially in initial state  $\hat{\rho}_0$ . A parameter-independent unitary transformation  $\hat{U}_1$  precedes the single channel invocation, producing a channel input state  $\hat{\rho}_i$ . A measurement follows the channel invocation.

### III. DEPOLARIZING-CHANNEL PARAMETER ESTIMATION: BACKGROUND AND BASELINES

The simplest parameter-estimation scheme, which also forms the baseline against which all other schemes may be compared, is that where the channel is invoked once on a single qubit and is described in Fig. 2. This will be termed the single-qubit, single-channel (SQSC) protocol.

The unitary  $\hat{U}_1$  of Fig. 2 changes only the orientation of  $\mathbf{r}$ , leaving the polarization unaltered, and thus can be omitted. Then Eq. (1) yields that the state after one channel invocation is  $\hat{\rho}_f = (\hat{I} + \lambda \mathbf{r} \cdot \hat{\boldsymbol{\sigma}})/2$ . The quantum Fisher information can be computed by first determining the SLD using Proposition 1 of [28] and then substituting into Eq. (9). This proposition (appropriately corrected) states that if  $\alpha := \text{Tr}(\hat{\rho}_f^2) - (\text{Tr} \hat{\rho}_f)^2 = 0$ , then  $\hat{L} = [2 \frac{\partial \hat{\rho}_f}{\partial \lambda} - \frac{\partial \ln |\text{Tr} \hat{\rho}_f|}{\partial \lambda} \hat{\rho}_f] / \text{Tr} \hat{\rho}_f$ , while if  $\alpha \neq 0$ , then  $\hat{L} = [2 \frac{\partial \hat{\rho}_f}{\partial \lambda} - \frac{\partial \ln |\alpha|}{\partial \lambda} \hat{\rho}_f] / \text{Tr} \hat{\rho}_f + \frac{\partial}{\partial \lambda} \ln (|\alpha| / \text{Tr} \hat{\rho}_f) \hat{I}$ . Straightforward calculation gives  $\text{Tr} \hat{\rho}_f = 1$  and  $\alpha = (\lambda^2 r^2 - 1)/2$ . The only circumstances under which  $\alpha = 0$  are when  $r = 1$  and  $\lambda = 1$ . We henceforth only consider  $\lambda < 1$ . It follows that for a single channel invocation on the state of Eq. (10) the SLD is

$$\hat{L} = -\frac{\lambda r^2}{1 - \lambda^2 r^2} \hat{I} + \frac{1}{1 - \lambda^2 r^2} \mathbf{r} \cdot \hat{\boldsymbol{\sigma}}. \quad (11)$$

Substituting into Eq. (9) then indicates that the quantum Fisher information for the SQSC protocol using an initial state with polarization  $r$  is

$$H_s(\lambda) = \frac{r^2}{1 - \lambda^2 r^2}. \quad (12)$$

This is the baseline quantum Fisher information against which all other estimation schemes are to be compared.

#### A. Pure-initial-state estimation schemes

We briefly digress to discuss the previously investigated [23–26] extreme case, where the initial states are pure. If it were possible to modify the initial-state polarization, then Eq. (12) shows that, in accordance with general results [23,40], the largest quantum Fisher information would be attained for a pure input state, i.e., when  $r = 1$ , giving

$$H_{\text{spure}}(\lambda) = \frac{1}{1 - \lambda^2}. \quad (13)$$

Usually, the key issue of interest in quantum parameter estimation is whether greater quantum Fisher information can be attained when entangled multiple qubits are available as input for the channel. For the depolarizing channel it has been shown that entanglement can yield greater quantum Fisher information. Specifically, if the channel is applied to one of two qubits, then the optimal quantum Fisher information is attained [23,26] when the two qubits are prepared in a maximally

entangled pure state, such as  $|\Psi_i\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ . The resulting quantum Fisher information is

$$H_{\text{pureopt}}(\lambda) = \frac{3}{(3 + \lambda)(1 - \lambda)}. \quad (14)$$

It is straightforward to show that  $H_{\text{pureopt}}(\lambda) > H_{\text{spure}}(\lambda)$  whenever  $\lambda > 0$ .

The remaining question is whether any additional qubits and channel invocations can yield greater quantum Fisher information per channel invocation. Remarkably, the result is [25] that the optimal depolarizing-channel parameter-estimation scheme uses pairs of qubits, each in a maximally entangled pure input state. The channel is applied once to only one qubit of each entangled pair, and the resulting quantum Fisher information per channel use is that of Eq. (14). Thus when qubits are available in pure initial states, entangling more than two qubits cannot yield any advantages for depolarizing-channel parameter estimation. However, we stress that this does not necessarily pertain to the situation that we address, in which the available input states are not pure.

#### IV. MULTIPLE CHANNEL USES: UNCORRELATED-STATE PROTOCOLS

The previous discussion motivates the central questions of our work: given a collection of qubits, each initially in a state with the same polarization  $r$ , is it possible to enhance the parameter-estimation accuracy by using multiple channel invocations or entanglement or correlations amongst more than two qubits? If so, to what extent can the accuracy, as measured by the quantum Fisher information per channel use, be enhanced?

A first strategy for enhancing estimation accuracy is one where the same process is repeated independently, as is done for classical repeat and average schemes. Specifically, we consider the protocol of Fig. 3, called the *independent channel use protocol*. Here there are  $m$  qubits, each in the initial state  $\hat{\rho}_0$  and subject to a parameter-independent single-qubit preparatory unitary. The channel is subsequently invoked exactly once on each qubit. In this protocol there are never any correlations between the qubits during the entire process; in this sense it resembles a classical approach.

The quantum Fisher information is additive in such cases [28,35], and thus the quantum Fisher information for the independent channel use protocol with  $m$  channel

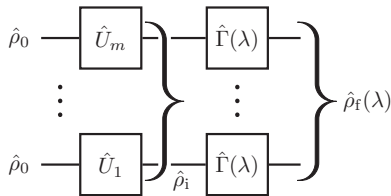


FIG. 3. Independent channel use protocol. There are  $m$  single qubits, each initially in the state  $\hat{\rho}_0$ . Qubit  $j$  is subjected to a single-qubit unitary  $\hat{U}_j$ , which is independent of the channel parameter, producing the input state  $\hat{\rho}_i$ . Thereafter a depolarizing channel is applied once to each qubit.

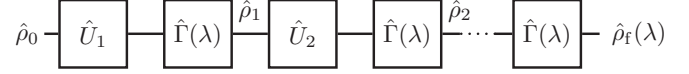


FIG. 4. Sequential channel-use protocol. A single qubit, initially in state  $\hat{\rho}_0$ , is subjected to  $m$  channel invocations. Each channel invocation is preceded by a single-qubit unitary,  $\hat{U}_1, \dots, \hat{U}_m$ , all of which are independent of the channel parameter.

invocations is

$$H(\lambda) = m H_s(\lambda) = \frac{m r^2}{1 - \lambda^2 r^2}. \quad (15)$$

Although this is an improvement over the SQSC protocol, clearly, the quantum Fisher information *per channel use* in the independent channel use protocol is identical to that of the SQSC protocol. Thus the independent channel use protocol attains the same estimation accuracy, measured in terms of quantum Fisher information per channel invocation, as the SQSC protocol.

A second strategy, illustrated in Fig. 4, is that where only one qubit is available and the channel is invoked sequentially a total of  $m$  times. Successive channel invocations are interspersed with parameter-independent unitaries. Assuming the standard initial state  $\hat{\rho}_0$ , the effect of  $\hat{U}_1$  is to rotate the polarization vector,  $\mathbf{r} \rightarrow \mathbf{r}_1$  without altering its magnitude. Then Eq. (1) implies that the state after the first channel invocation is  $\hat{\rho}_1 = (\hat{I} + \lambda \mathbf{r}_1 \cdot \hat{\boldsymbol{\sigma}})/2$ . Using the same argument, the state after the second channel invocation is  $\hat{\rho}_2 = (\hat{I} + \lambda^2 \mathbf{r}_2 \cdot \hat{\boldsymbol{\sigma}})/2$ , where  $\hat{U}_2$  rotates  $\mathbf{r}_1 \rightarrow \mathbf{r}_2$ . Continuing, the state prior to measurement is  $\hat{\rho}_f = (\hat{I} + \lambda^m \mathbf{r}_f \cdot \hat{\boldsymbol{\sigma}})/2$ , where  $r_f = r$ . A calculation similar to that giving Eq. (12) indicates that the quantum Fisher information for  $m$  sequential channel invocations on a single qubit is

$$H_{\text{seq}}(\lambda) = m^2 \frac{\lambda^{2m-2} r^2}{1 - \lambda^{2m} r^2}. \quad (16)$$

Thus the quantum Fisher information per channel invocation is

$$H_{\text{seq/channel}}(\lambda) = m \frac{\lambda^{2m-2} r^2}{1 - \lambda^{2m} r^2}. \quad (17)$$

To compare this to the SQSC protocol we define the *sequential channel use gain* as

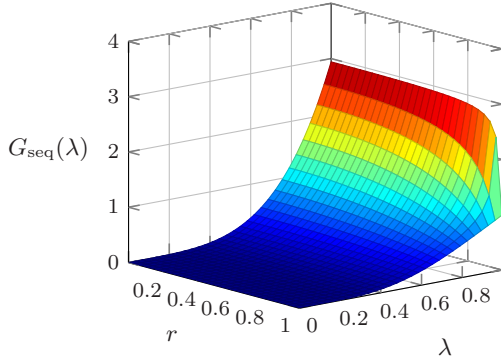
$$G_{\text{seq}}(\lambda) := \frac{H_{\text{seq/channel}}(\lambda)}{H_s(\lambda)} = m \frac{\lambda^{2m-2} - \lambda^{2m} r^2}{1 - \lambda^{2m} r^2}. \quad (18)$$

Figure 5 illustrates the typical gain, plotted here for the  $m = 3$  case. This shows that the sequential channel use protocol is advantageous for certain ranges of parameter values and polarizations but disadvantageous for others.

The sequential channel use gain decreases monotonically with  $r$  and increases monotonically with  $\lambda$  (these are proved in Appendix A). A more detailed analysis of this separates the pure-initial-state case, i.e.,  $r = 1$ , from mixed-initial-state cases, i.e.,  $r < 1$ . For the pure-initial-state case, it is shown in Appendix A that

$$0 \leq G_{\text{seq}}(\lambda) \leq 1. \quad (19)$$



FIG. 5. (Color online) Sequential channel use gain for  $m = 3$ .

For the mixed-initial-state case, it is also shown in Appendix A that

$$0 \leq G_{\text{seq}}(\lambda) \leq m. \quad (20)$$

In both cases the upper bound is attained when  $\lambda = 1$ .

It follows that if the available initial state is pure, there is no advantage to the sequential channel use protocol. If the available initial state is mixed, then, for certain initial polarizations and the parameter values, there can be an advantage to the sequential channel use protocol.

It remains to assess whether for mixed initial states there is any advantage to increasing the number of channel invocations. To do so, we compare the quantum Fisher information per channel use of Eq. (17) for  $m + 1$  channel invocations versus that for  $m$  channel invocations. An advantage is attained when the ratio of that for  $m + 1$  to that for  $m$  exceeds 1, and straightforward algebra shows that this is equivalent to  $r^2 \leq [\lambda^2(m + 1) - m]/\lambda^{2m+2}$ . The right-hand side of this increases monotonically with  $\lambda$  and attains a maximum of 1 when  $\lambda = 1$ . Also it is negative when  $\lambda < \sqrt{m/(m + 1)}$ , implying that when  $\lambda < \sqrt{m/(m + 1)}$ , there is no polarization for which an additional channel use will give an advantage. Thus for any polarization there will be some parameter values for which additional invocations in the sequential channel use protocol will be advantageous. However, the range of possible parameter values for which this occurs, bounded from below by at least  $\sqrt{m/(m + 1)}$ , shrinks with increasing channel invocations.

## V. MULTIPLE QUBITS OR CHANNEL USES: CORRELATED-STATE PROTOCOL

An additional resource available to multiple-qubit systems is the existence of states in which there are correlations between the individual qubits, and we now consider whether these can enhance the accuracy of parameter estimation for the depolarizing channel.

We consider the particular correlated-state protocol procedure in Fig. 6; this was previously investigated for other channels [27,28]. We assume that each qubit is initially in the particular state  $\hat{\rho}_0 = (\hat{I} + r\hat{\sigma}_y)/2$  with polarization  $r$  and that a preparatory unitary  $\hat{U}_{\text{prep}}$ , illustrated in Fig. 7, is subsequently applied jointly to the qubits. Denote the density operator for the system after the preparatory gate by  $\hat{\rho}_i := \hat{U}_{\text{prep}}\hat{\rho}_i\hat{U}_{\text{prep}}^\dagger$ . It

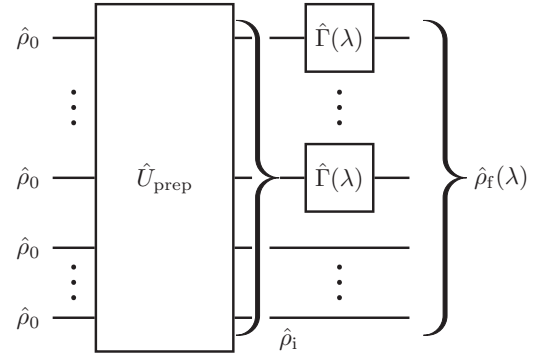


FIG. 6. Correlated-state protocol considered in this article. There are  $n$  single qubits, each initially in state  $\hat{\rho}_0$ . These are subjected to a joint preparatory unitary  $\hat{U}_{\text{prep}}$ , producing the channel input state  $\hat{\rho}_i$ . Thereafter a depolarizing channel is applied once to each of the uppermost  $m$  qubits. The preparatory unitary is illustrated in Fig. 7.

can be shown [28] that

$$\hat{\rho}_i = \sum_{x=0}^{(N-1)/2} \hat{\rho}_x, \quad (21)$$

where  $N = 2^n - 1$  and

$$\hat{\rho}_x = d_{j(x)}[|x\rangle\langle x| + |N - x\rangle\langle N - x|] + ic_{j(x)}[|x\rangle\langle N - x| - |N - x\rangle\langle x|]. \quad (22)$$

The counterdiagonal terms of the resulting matrix of Eq. (22) are constructed by first computing the number of zeros  $j(x)$  in the binary representation  $x_n \cdots x_1$  for  $x$  and then using

$$c_j = \frac{1}{2^{n+1}} [(1 + r)^j(1 - r)^{n-j} - (1 + r)^{n-j}(1 - r)^j]. \quad (23)$$

The diagonal terms are

$$d_j = \frac{1}{2^{n+1}} [(1 + r)^j(1 - r)^{n-j} + (1 + r)^{n-j}(1 - r)^j]. \quad (24)$$

As described previously [28], this scheme results in a density operator which has supports consisting of mutually orthogonal two-dimensional subspaces; in terms of matrix representations it can be expressed as a sum of  $2 \times 2$  matrices acting on distinct vector spaces.

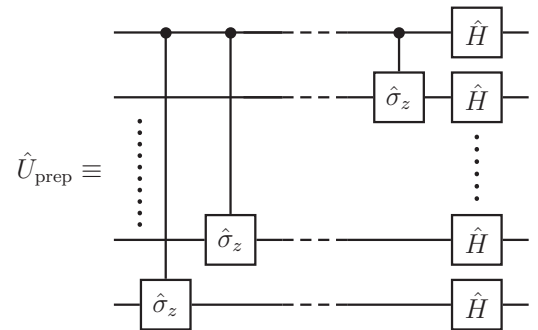


FIG. 7. The preparatory gate  $\hat{U}_{\text{prep}}$  consists of a collection of controlled-Z operations applied to each distinct pair of qubits followed by a Hadamard transformation applied to each qubit.

When the initial states are pure, i.e.,  $r = 1$ , the diagonal and counterdiagonal terms are all zero except  $c_0 = -c_n = -1/2$  and  $d_0 = d_n = 1/2$ , and  $\hat{\rho}_i$  is the density operator corresponding to the Greenberger-Horne-Zeilinger-type state  $(|0 \dots 0\rangle + |1 \dots 1\rangle)/\sqrt{2}$ .

Suppose that the channel acts once on each of  $m$  qubits corresponding to the least significant (or rightmost) digits in the computational basis representation. The action of the channel on multiple qubits is readily described by noting that Eq. (1) implies that, for a single qubit,

$$|x\rangle\langle y| \xrightarrow{\hat{r}(\lambda)} \lambda |x\rangle\langle y|, \quad (25a)$$

$$|x\rangle\langle x| \xrightarrow{\hat{r}(\lambda)} p|x\rangle\langle x| + q|\bar{x}\rangle\langle \bar{x}|, \quad (25b)$$

where  $|x\rangle$  and  $|y\rangle$  are computational basis states such that  $x \neq y$  and  $\bar{x} := 1 - x$ . Here  $p := (1 + \lambda)/2$  and  $q := (1 - \lambda)/2$ . A general state of multiple qubits can be expressed in terms of linear combinations and tensor products of basic operators such as  $|x\rangle\langle y|$ , and thus Eqs. (25) can be used to describe the action of any number of channels acting on multiple qubits.

Equation (25a) implies the counterdiagonal terms of the matrix representing  $\hat{\rho}_f(\lambda)$  are attained from those of  $\hat{\rho}_i$  by multiplication by  $\lambda^m$ . Equation (25b) implies that the diagonal terms of the matrix representing  $\hat{\rho}_f(\lambda)$  result from rearrangements of those of  $\hat{\rho}_i$  multiplied by various factors of  $p$  and  $q$ . The remaining terms are again all zero. An additional simplification, demonstrated in Appendix B, is that  $\langle N - x | \hat{\rho}_f(\lambda) | N - x \rangle = \langle x | \hat{\rho}_f(\lambda) | x \rangle$ . Thus the final density operator has a form similar to that for  $\hat{\rho}_i$ , i.e.,

$$\hat{\rho}_f(\lambda) = \sum_{x=0}^{(N-1)/2} \hat{\rho}_{f,x}, \quad (26)$$

where

$$\begin{aligned} \hat{\rho}_{f,x} = & d_{f,x} [|x\rangle\langle x| + |N - x\rangle\langle N - x|] \\ & + i c_{f,x} [|x\rangle\langle N - x| - |N - x\rangle\langle x|]. \end{aligned} \quad (27)$$

Equation (25a) yields

$$c_{f,x} = \lambda^m c_{j(x)} \quad (28)$$

for the counterdiagonal terms, where  $j(x)$  is the number of zeros in the bit string for  $x$ .

Determining the diagonal terms is further simplified by noting that the preparatory unitary is invariant under interchange of any two qubits and that this is also true of the channel operation provided that the channel either acts on each qubit that is interchanged or that it acts on neither of the qubits that are interchanged. The invariance of the preparatory unitary is readily apparent from its structure, as shown in Fig. 7. More precisely, suppose that  $\hat{S}_{j'j}$  is the unitary operation which swaps the qubits labeled  $j$  and  $j'$ . Then if  $1 \leq j < j' \leq m$  (recall that the channel acts on the rightmost  $m$  bits),

$$\langle y | \hat{S}_{j'j}^\dagger \hat{\rho}_f \hat{S}_{j'j} | x \rangle = \langle y | \hat{\rho}_f | x \rangle, \quad (29)$$

with an identical result when  $m + 1 \leq j < j' \leq n$ . Thus if the bit string for  $x$  is  $x_n \dots x_{m+1} x_m \dots x_1$ , then  $d_{f,x} = \langle x | \hat{\rho}_f | x \rangle$  is invariant under the interchange of any two of  $\{x_n, \dots, x_{m+1}\}$  and is also invariant under the interchange

any two of  $\{x_m, \dots, x_1\}$  (it is not, in general, invariant under interchanges between one element from one of these sets and another from the other set). For example, if the channel is applied, the two least significant qubits out of a total of five qubits is then  $d_{f,6} = d_{f,5}$  (or, using a binary representation for the index subscript,  $d_{f,00110} = d_{f,00101}$ ) and  $d_{f,26} = d_{f,21}$  (or  $d_{f,11010} = d_{f,10101}$ ). A consequence of this is that  $d_{f,x}$  depends on only the number of zeros in the leftmost  $n - m$  bits of the binary representation of  $x$  and also the number of zeros in the rightmost  $m$  bits of the binary representation of  $x$ . This consideration and a derivation, provided in Appendix C, yield

$$d_{f,x} = \sum_{k=0}^m q^k p^{m-k} \sum_{l=l_{\min}}^{l_{\max}} \binom{v}{l} \binom{m-v}{k-l} d_{u+v+k-2l}, \quad (30)$$

where  $u = u(x)$  is the number of zeros in the leftmost  $n - m$  bits (i.e.,  $x_n, \dots, x_{m+1}$ ) of the binary representation of  $x$ ,  $v = v(x)$  is the number of zeros in the rightmost  $m$  bits (i.e.,  $x_m, \dots, x_1$ ) of the binary representation of  $x$ ,  $l_{\min} = \max(k + v - m, 0)$ , and  $l_{\max} = \min(k, v)$ . Clearly,  $d_{f,x}$  depends on  $u, v$ , and  $m$  and  $\lambda$ , via  $p = (1 + \lambda)/2$  and  $q = (1 - \lambda)/2$ . Since  $\lambda$  is implicit throughout this work and  $m$  is fixed by the number of channel invocations, we will find it convenient to express  $d_{f,x}$  as  $d_{f,x} = d_f(u, v)$ .

According to Eqs. (26) and (27),  $\hat{\rho}_f$  is a sum of operators, each acting on a two-dimensional space, which have mutually orthogonal supports. Thus Proposition 2 of [28] implies that the quantum Fisher information is

$$H_{\text{corr}}(\lambda) = \sum_{x=0}^{(N-1)/2} H_x(\lambda), \quad (31)$$

where  $H_x(\lambda)$  is the quantum Fisher information associated with  $\hat{\rho}_{f,x}$ . A derivation (see Appendix D) based on this and Eq. (8) yields

$$\begin{aligned} H_{\text{corr}}(\lambda) = & \sum_{x=0}^{(N-1)/2} \frac{2}{d_{f,x}^2 - \lambda^{2m} c_{j(x)}^2} \\ & \times [d_{f,x} (\dot{d}_{f,x}^2 + m^2 \lambda^{2m-2} c_{j(x)}^2) - 2m \lambda^{2m-1} \dot{d}_{f,x} c_{j(x)}^2], \end{aligned} \quad (32)$$

where the dot indicates differentiation with respect to  $\lambda$ . Although the sum in Eq. (32) is over  $x$ , the terms indexed as such depend on  $u$  and  $v$ , and it follows that the quantum Fisher information can be expressed as a sum over these. In Appendix D it is shown that if  $m < n$ , then

$$\begin{aligned} H_{\text{corr}}(\lambda) = & \sum_{v=0}^m \sum_{u=1}^{n-m} \binom{n-m-1}{u-1} \binom{m}{v} \frac{2}{d_f^2 - \lambda^{2m} c_{u+v}^2} \\ & \times [d_f (\dot{d}_f^2 + m^2 \lambda^{2m-2} c_{u+v}^2) - 2m \lambda^{2m-1} \dot{d}_f c_{u+v}^2], \end{aligned} \quad (33)$$

where  $d_f = d_f(u, v)$  is given by Eq. (30). If  $n = m$ , then

$$\begin{aligned} H_{\text{corr}}(\lambda) = & \sum_{v=1}^n \binom{n-1}{v-1} \frac{2}{d_f^2 - \lambda^{2m} c_v^2} \\ & \times [d_f (\dot{d}_f^2 + m^2 \lambda^{2m-2} c_v^2) - 2m \lambda^{2m-1} \dot{d}_f c_v^2], \end{aligned} \quad (34)$$

where  $d_f = d_f(0, v)$  is again given by Eq. (30). In both cases  $c_j$  is given by Eq. (23). These represent the simplest expressions that we have been able to obtain for the quantum Fisher information for the correlated-state protocol.

The quantum Fisher information per channel invocation is

$$H_{\text{corr/channel}}(\lambda) = \frac{H_{\text{corr}}(\lambda)}{m}. \quad (35)$$

We aim to compare the performance of the correlated-state protocol to that of the SQSC protocol in terms of the quantum Fisher information per channel use and given that the initial qubit polarizations are the same. We define the correlated-state protocol quantum Fisher information gain as

$$G_{\text{corr}}(\lambda) := \frac{H_{\text{corr/channel}}(\lambda)}{H_s(\lambda)}, \quad (36)$$

and whenever this exceeds 1, the correlated-state protocol outperforms the SQSC protocol.

The expression for the quantum Fisher information is a rational polynomial in  $r$  and  $\lambda$ , and even with as few as two qubits, this is too complicated to yield insight into the estimation accuracy for the correlated-state protocol for all values of polarization and the parameter. While the same applies to the gain, aspects of its behavior can be illustrated graphically.

First, suppose that there is only one channel invocation ( $m = 1$ ). Figure 8 illustrates the gain for the examples  $n = 2$

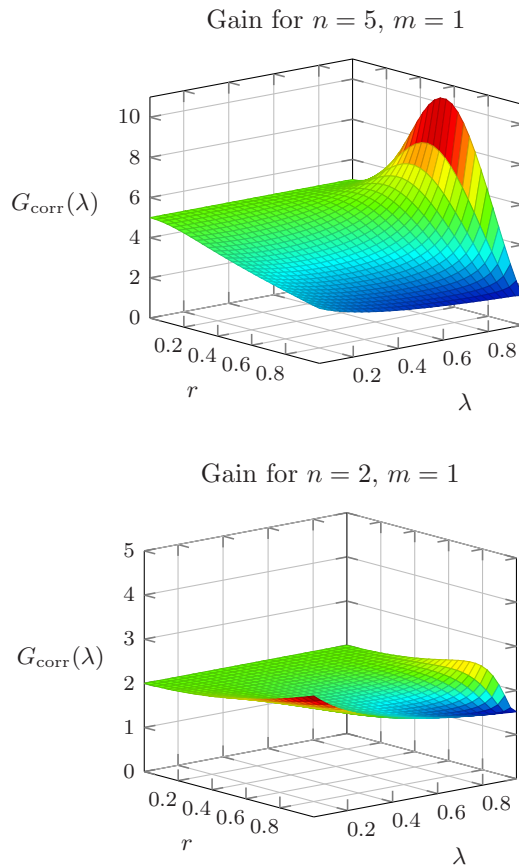


FIG. 8. (Color online) Gain using one channel invocation. Both plots are over the range  $0.05 \leq \lambda \leq 0.95$  and  $0 \leq r \leq 1$ .

and  $n = 5$ . These suggest that when the channel is invoked only once, the correlated-state protocol will be more accurate than the SQSC protocol, assuming the same initial-state polarization for both. However, a general proof of this is elusive; the methods of [28] used to prove a similar fact for the phase-flip channel are not immediately applicable here.

Second, suppose that there are multiple channel invocations ( $m > 1$ ). Figure 9 illustrates the correlated-state gain of Eq. (36) for various numbers of channel invocations on four qubits. These show that when the channel is invoked multiple times, there are polarizations and parameter values for which

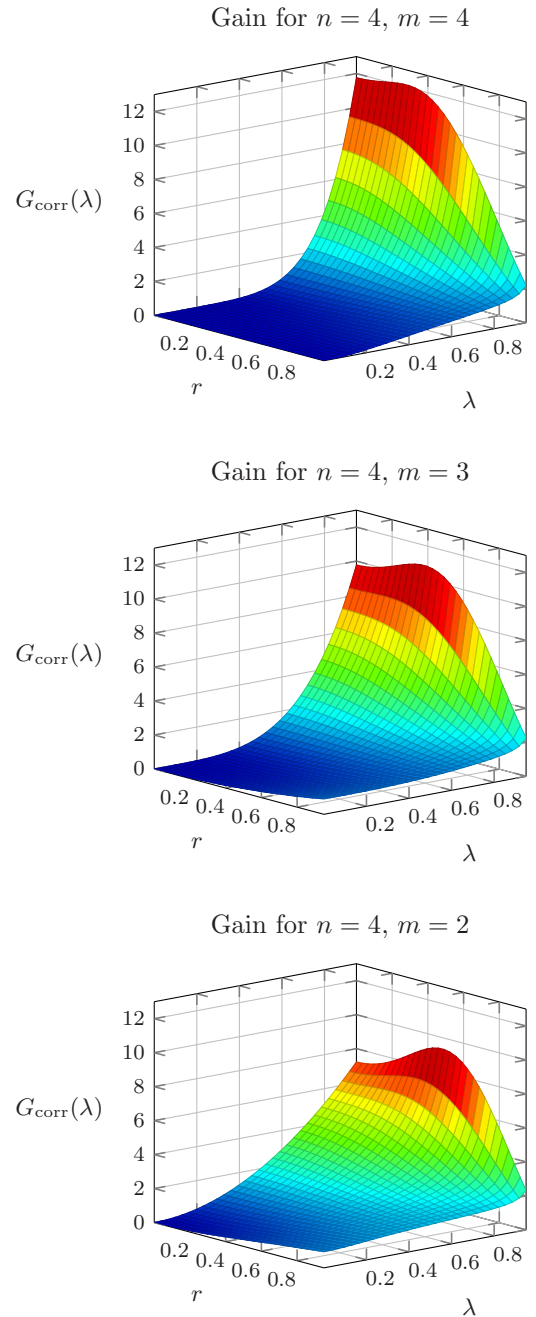


FIG. 9. (Color online) Gain using multiple-channel invocations on four qubits. All plots are over the range  $0 \leq \lambda, r \leq 0.95$ .

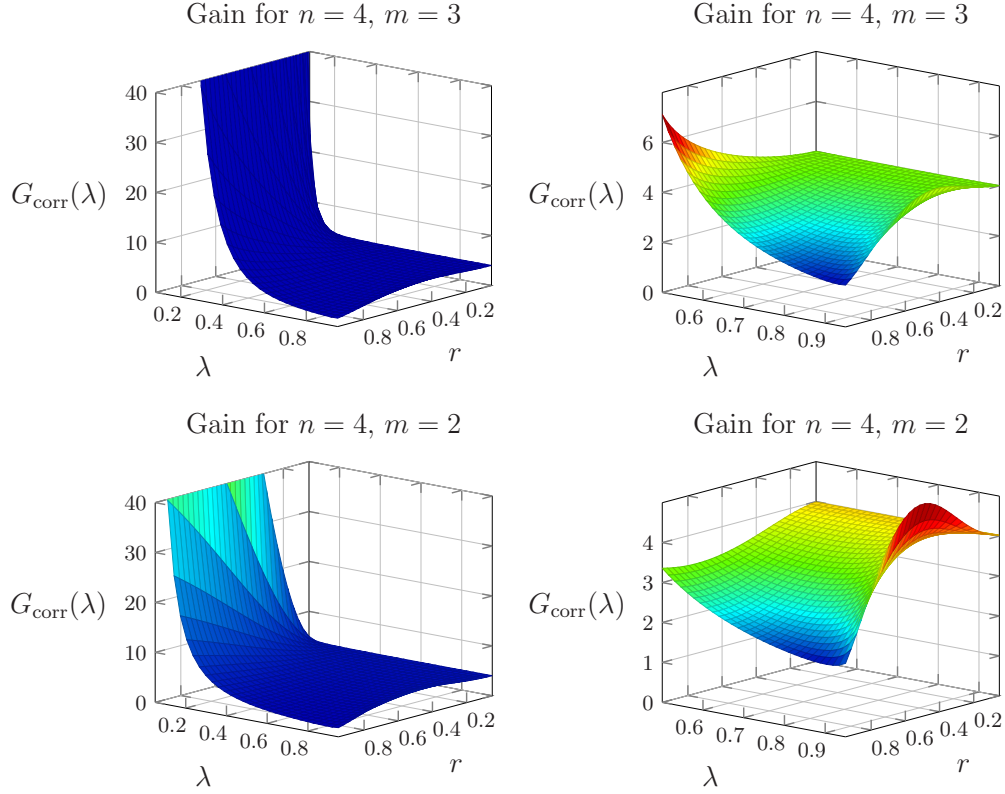


FIG. 10. (Color online) Correlated vs sequential channel gain using multiple-channel channel invocations on four qubits. Plots on the left are over the range  $0.05 \leq \lambda, r \leq 0.95$ . Plots on the right provide details for  $\lambda \geq 0.5$ .

the correlated-state protocol will be more accurate than the SQSC protocol, but there are also parameter values for which it is inferior.

Given that the channel is invoked multiple times, the correlated-state protocol can also be compared to the sequential channel protocol that uses the same number of channel invocations. We define the correlated vs sequential channel gain as

$$G_{\text{corr/seq}}(\lambda) := \frac{H_{\text{corr/channel}}(\lambda)}{H_{\text{seq/channel}}(\lambda)}, \quad (37)$$

where the number of channel invocations is the same for the two protocols.

Figure 10 suggests that when the channel is invoked a fixed number of times, the correlated-state protocol is more accurate than the sequential protocol, using the same number of channel invocations, over all parameter values and for all polarizations.

## VI. WEAK INITIAL POLARIZATION CASES

In some situations the initial-state polarization is very small, i.e.,  $r \ll 1$ . This is true of room-temperature solution-state NMR [14], where typically  $r \approx 10^{-4}$ .

When  $r \ll 1$ , the SQSC protocol quantum Fisher information becomes

$$H_s(\lambda) \approx r^2, \quad (38)$$

and the sequential-channel-use-protocol quantum Fisher information per channel use becomes

$$H_{\text{seq/channel}}(\lambda) \approx m\lambda^{2m-2}r^2, \quad (39)$$

each to lowest order in  $r$ . In Appendix E we show that the correlated-state quantum Fisher information per channel use becomes

$$H_{\text{corr/channel}}(\lambda) \approx mn\lambda^{2m-2}r^2 \quad (40)$$

to lowest order in  $r$ .

Here the sequential channel use gain approximates to

$$G_{\text{seq}}(\lambda) \approx m\lambda^{2m-2}. \quad (41)$$

Equation (41) shows that the gain exceeds 1 when the depolarizing-channel parameter satisfies  $\lambda \geq \lambda_{\text{cutoff}}(m)$ , where  $\lambda_{\text{cutoff}}(m) := m^{1/(2-2m)}$  is the characteristic parameter cutoff. The characteristic parameter cutoff, plotted in Fig. 11, is a monotonically increasing function of  $m$ , with a minimum value of  $e^{-1/2} = 0.61$ , attained as  $m \rightarrow 1$ , and a maximum value of 1, attained as  $m \rightarrow \infty$ . This indicates that for any given parameter value, there will be a maximum number of channel invocations beneath which the sequential channel use protocol offers enhanced parameter-estimation accuracy and beyond which it will not do so. Figure 11 shows that as  $\lambda$  increases, accuracy gains will persist with an increasing number of channel invocations. Note that the larger  $\lambda$  is, the weaker the depolarization is, and for such weak depolarization cases enhanced estimation accuracies can be attained with multiple



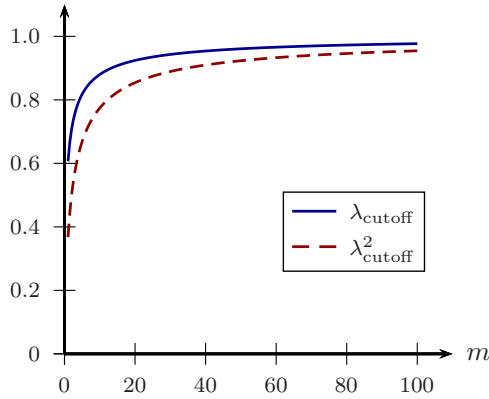


FIG. 11. (Color online) Parameter cutoff function and its square vs  $m$ .

sequential channel invocations. Thus, for low polarizations, the sequential channel use protocol can yield a greater estimation accuracy per channel invocation than the SQSC protocol. However, this requires that the parameter value exceed the characteristic parameter cutoff, and Fig. 11 indicates that such advantages will be absent for low enough parameter values and, even when there is an advantage, increasing the number of channel invocations will eventually eliminate this advantage.

The correlated-state-protocol gain (versus the SQSC protocol) approximates to

$$G_{\text{corr}}(\lambda) \approx mn\lambda^{2m-2}. \quad (42)$$

We consider two cases separately.

First, with only one channel invocation the correlated-state protocol offers an  $n$ -fold gain in accuracy regardless of the parameter value for low initial polarization states. This is strikingly different from the pure-state case where the optimal accuracy is attained [25] with a single channel invocation on one of only two qubits ( $n = 2$  and  $m = 1$ ); by contrast, when the initial-state polarization is low and the channel is invoked on only one qubit, then adding more qubits always increases the estimation accuracy.

Second, with multiple channel invocations, Eq. (42) indicates that enhanced estimation accuracy will occur if  $\lambda \geq (mn)^{1/(2-2m)} = \lambda_{\text{cutoff}}(m) n^{1/(2-2m)}$ . The right-hand side forms a new cutoff which is again an increasing function of the number of channel invocations but a decreasing function of the total number of qubits. Thus increasing the number of spectator qubits while leaving the number of channel invocations fixed extends the range of parameter values over which the correlated-state protocol is advantageous. Furthermore Eq. (42) shows that adding more spectator qubits while keeping the number of channel invocations fixed will increase the quantum Fisher information per channel use; the increase can be arbitrarily large by adding sufficiently many spectator qubits. Unlike the pure-initial-state case, for low-polarization initial states, there will always be an advantage to adding additional spectator qubits.

Separately, when  $m < n$ , we can assess whether one additional channel invocation yields any advantage. Equation (40) implies that starting with  $m$  channel invocations and adding one more invocation increases the quantum Fisher information

TABLE I. Optimal number of correlated-state-protocol channel invocations and optimal gain, i.e., Eq. (42) evaluated at  $m_{\text{opt}}$ , whenever  $m < n$ .

$\lambda$	$m_{\text{opt}}$	Optimal gain
0.700	1	1.00 $n$
0.800	2	1.28 $n$
0.900	5	2.15 $n$
0.950	10	3.97 $n$
0.990	50	18.67 $n$
0.995	100	37.07 $n$

if  $m < \lambda^2/(1 - \lambda^2)$ , decreases it if  $m > \lambda^2/(1 - \lambda^2)$ , and makes no difference if  $m = \lambda^2/(1 - \lambda^2)$ . Thus the optimal number of channel invocations in the correlated-state protocol is  $m_{\text{opt}} = \lfloor \lambda^2/(1 - \lambda^2) \rfloor + 1$ , unless  $\lambda^2/(1 - \lambda^2)$  is an integer, in which case,  $m_{\text{opt}} = \lambda^2/(1 - \lambda^2)$ . Examples of this and the associated gains are provided in Table I. When  $\lambda$  is close enough to 1, this offers considerable opportunity for improved accuracy. Again, unlike the pure-initial-state case, for low initial polarization, increasing the number of channel invocations in the correlated-state protocol can result in enhanced estimation accuracy per channel use.

In many physical situations every qubit is subjected to the depolarizing channel. When the channel is invoked on all qubits of the correlated-state protocol ( $m = n$ ), the gain becomes  $G_{\text{corr}}(\lambda) \approx m^2 \lambda^{2m-2}$ , and this implies that the correlated-state protocol provides enhanced accuracy whenever  $\lambda \geq \lambda_{\text{cutoff}}^2(m)$ . This lower bound is plotted in Fig. 11. This is again an increasing function of  $m$ , approaching  $e^{-1} = 0.37$  as  $n = m \rightarrow 1$ . The slightly lower cutoff implies that there is somewhat greater scope for enhanced parameter estimation when all qubits are subjected to the channel. However, for a given parameter value, this cutoff establishes an upper bound on the number of qubits and channel invocations for which the correlated-state protocol provides any gain.

We can again ask when adding one more qubit and channel invocation gives any advantage. Equation (42) with  $m = n$  implies that if there are originally  $m$  channel invocations, then adding one more gives greater quantum Fisher information per channel use if  $m \leq m_{\text{opt}}$ , where  $m_{\text{opt}} = \lfloor \lambda/(1 - \lambda) \rfloor + 1$  unless  $\lambda/(1 - \lambda)$  is an integer, in which case,  $m_{\text{opt}} = \lambda/(1 - \lambda)$ . Examples of this and the associated optimal gains are provided in Table II. Clearly, for relatively weak depolarizing channels,

TABLE II. Optimal number of correlated-state-protocol channel invocations and optimal gain, i.e., Eq. (42) evaluated at  $m_{\text{opt}}$ , whenever the channel is invoked once on each qubit ( $m = n$ ).

$\lambda$	$m_{\text{opt}}$	Optimal gain
0.500	1	1.00
0.700	3	2.16
0.900	9	15.01
0.950	19	56.96
0.970	33	155.03
0.990	100	1367.00

i.e.,  $\lambda \approx 1$ , substantial enhancements of estimation accuracy are possible with the correlated-state protocol.

Finally, the correlated-state protocol and sequential channel protocol can be compared in the low initial polarization limit, given the same number of channel invocations. Here the correlated vs sequential channel gain is

$$G_{\text{corr/seq}}(\lambda) \approx n, \quad (43)$$

and thus when  $r \ll 1$ , the correlated-state protocol will always offer a better estimation accuracy than the sequential channel protocol provided that the number of channel invocations for each is the same.

## VII. QUANTUM CORRELATIONS IN THE CORRELATED-STATE PROTOCOL

The presence of quantum correlations such as entanglement or discord in the correlated-state protocol may be assessed for  $n = 2$  along the same lines as was done for the Pauli channel parameter estimation of [28]. Then Eqs. (27), (28), and (30) yield, with  $m$  channel invocations,

$$\hat{\rho}_f = \frac{1}{4} \begin{pmatrix} 1 + \lambda^m r^2 & 0 & 0 & 2ir\lambda^m \\ 0 & 1 - \lambda^m r^2 & 0 & 0 \\ 0 & 0 & 1 - \lambda^m r^2 & 0 \\ -2ir\lambda^m & 0 & 0 & 1 + \lambda^m r^2 \end{pmatrix} \quad (44)$$

in the computational basis. The state of the system prior to channel invocation can be obtained from this by setting  $\lambda = 1$ .

The presence of entanglement can be assessed by considering partial transpose of  $\hat{\rho}_f$ , and this is

$$\hat{\rho}_f^{\text{PT}} = \frac{1}{4} \begin{pmatrix} 1 + \lambda^m r^2 & 0 & 0 & 0 \\ 0 & 1 - \lambda^m r^2 & 2ir\lambda^m & 0 \\ 0 & -2ir\lambda^m & 1 - \lambda^m r^2 & 0 \\ 0 & 0 & 0 & 1 + \lambda^m r^2 \end{pmatrix}. \quad (45)$$

The state is separable if  $\hat{\rho}_f^{\text{PT}}$  is positive [44,45]. The eigenvalues of this will be positive if and only if  $0 \leq r \leq \sqrt{1 + 1/\lambda^m} - 1$ . Thus the state prior to channel invocation will be separable if and only if  $0 \leq r \leq \sqrt{2} - 1$ . The correlated-state protocol can give estimation gains as  $r \rightarrow 0$ , and this clearly corresponds to a state which is separable throughout the protocol. Thus the correlated-state-protocol gains cannot always be ascribed to the presence of entanglement.

Quantum discord describes correlations between quantum systems in terms of mutual information and measures the extent to which these exceed any possible classical correlations between the systems [27,46]. It is possible to compute the quantum discord for states with the form [47,48]

$$\hat{\rho} = \frac{1}{4} \left( \hat{I} + \sum_{j=1}^3 c_j \hat{\sigma}_j \otimes \hat{\sigma}_j \right), \quad (46)$$

where  $c_j$  are all real and  $\hat{\sigma}_1 = \hat{\sigma}_x, \dots$ . Defining

$$\lambda_0 := 1 - c_1 - c_2 - c_3, \quad (47a)$$

$$\lambda_1 := 1 - c_1 + c_2 + c_3, \quad (47b)$$

$$\lambda_2 := 1 + c_1 - c_2 + c_3, \quad (47c)$$

$$\lambda_3 := 1 + c_1 + c_2 - c_3, \quad (47d)$$

and

$$c := \max \{|c_1|, |c_2|, |c_3|\} \quad (48)$$

yields that the quantum discord is [47]

$$\mathcal{Q}(\hat{\rho}) = \frac{1}{4} \sum_{j=0}^3 \lambda_j \log_2 \lambda_j - \frac{1-c}{2} \log_2 (1-c) - \frac{1+c}{2} \log_2 (1+c). \quad (49)$$

Following the scheme of [28], the final density operator can be brought into the form of Eq. (46) by applying the single-qubit unitary

$$\hat{U} = \begin{pmatrix} 0 & e^{i\pi/8} \\ e^{-i\pi/8} & 0 \end{pmatrix} \quad (50)$$

to each qubit, and this will not alter the discord. Then

$$\lambda_0 = 1 - \lambda^m r^2, \quad (51)$$

$$\lambda_1 = 1 + 2r\lambda^m + \lambda^m r^2, \quad (52)$$

$$\lambda_2 = 1 - 2r\lambda^m + \lambda^m r^2, \quad (53)$$

$$\lambda_3 = 1 - \lambda^m r^2, \quad (54)$$

and

$$c = \max \{\lambda^m r^2, \lambda^m r\} = \lambda^m r \quad (55)$$

since  $0 \leq r \leq 1$ . Again, the discord for the correlated-state protocol prior to channel invocation can be determined by setting  $\lambda = 1$  and this gives

$$\mathcal{Q}(\hat{\rho}) = \frac{1+r}{2} \log_2 (1+r) + \frac{1-r}{2} \log_2 (1-r). \quad (56)$$

Then  $\frac{\partial \mathcal{Q}}{\partial r} > 0$  whenever  $r > 0$  and  $\mathcal{Q} = 0$  when  $r = 0$  imply that the state prior to channel invocation has nonzero discord whenever the polarization of each qubit is nonzero. In this sense, we can regard the correlated-state protocol as using states that have quantum correlations.

## VIII. DISCUSSION

We have considered estimation of the depolarizing-channel parameter for various situations where the available initial state of each qubit is mixed, and we quantified the accuracy of each in terms of the quantum Fisher information after channel invocation. We showed that for certain ranges of initial-state polarization and channel parameter, a protocol that uses correlated states prior to channel invocation attains

greater quantum Fisher information per channel invocation than either a protocol which uses product states throughout or another protocol which uses a sequence of channel invocations on a single qubit. For qubits with small initial polarizations we showed that using more than two qubits and more than two channel invocations can be advantageous; this is in contrast to the situation where qubits in pure initial states are available.

Our results suggest that, as with Pauli channel parameter estimation, a single invocation of the channel on many correlated qubits gives gains for all parameter values and initial polarizations. We were able to prove this only for the depolarizing channel in the limit as the initial polarization approaches zero, but we were also unable to generate a counterexample. This was not central to our results, but it does merit further investigation.

It is noteworthy that when the initial polarization is very small, the expression for the correlated-state-protocol quantum Fisher information, Eq. (40), is much simpler than those for the general initial polarization case, Eq. (33) or Eq. (34), and this results in a much simpler expression for correlated-state-protocol gain. A similar situation arose for Pauli channel parameter estimation [28]. The depolarizing and Pauli channels also share the result that, for low initial polarizations, the gain can be substantially larger than for pure-initial-state cases. This raises the question of whether these facts are true for any quantum channel when using a correlated-state protocol for low-polarization initial states. This and the question of whether such results can be derived without the degree of complication that appears in the general initial polarization case remain to be investigated.

The source of the gain cannot always be attributed to the presence of entangled or nonseparable states prior to channel invocation; we demonstrated this for the two-qubit example. We also showed that there is nonzero discord present prior to channel invocation in this example. A full analysis of the evolution of the discord and its possible relationship to gains in the quantum Fisher information might provide insight into the source of these accuracy gains; this is beyond the scope of our article and remains to be investigated.

Finally, we chose one particular preparatory unitary transformation for the analysis of the correlated-state protocol; that this yields gains in some cases is interesting enough. However, it is unclear whether this is optimal or whether there exists another parameter-independent unitary that offers greater gains.

#### APPENDIX A: SEQUENTIAL CHANNEL USE GAIN

The behavior of  $G_{\text{seq}}(\lambda)$  with respect to  $r$  can be assessed by first setting  $x := r^2$ . Then

$$G_{\text{seq}}(\lambda) = m \frac{\lambda^{2m-2} - \lambda^{2m} x}{1 - \lambda^{2m} x} \quad (\text{A1})$$

gives

$$\frac{\partial G_{\text{seq}}(\lambda)}{\partial x} = -m\lambda^{2m} \frac{1 + \lambda^{2m-2}}{(1 - \lambda^{2m} x)^2} \leq 0. \quad (\text{A2})$$

Since  $r$  increases as  $x$  increases, this proves the fact that  $G_{\text{seq}}(\lambda)$  is a monotonically decreasing function of  $r$ .

To assess the behavior of  $G_{\text{seq}}(\lambda)$  with respect to  $\lambda$ , let  $y := 1/\lambda^2$  and note that  $1 \leq y$ . Then

$$G_{\text{seq}}(\lambda) = m \frac{y - r^2}{y^m - r^2} \quad (\text{A3})$$

and

$$y^m - r^2 = (y - r^2) \sum_{k=0}^{m-1} y^k r^{2m-2k-2} + r^{2m} - r^2. \quad (\text{A4})$$

Thus

$$G_{\text{seq}}(\lambda) = \frac{m}{\sum_{k=0}^{m-1} y^k r^{2m-2k-2} + (r^{2m} - r^2)/(y - r^2)}. \quad (\text{A5})$$

The term  $(r^{2m} - r^2)/(y - r^2)$  is negative since  $0 \leq r \leq 1$  and  $1 \leq y$  and thus decreases as  $y$  increases. The remaining term  $\sum_{k=0}^{m-1} y^k r^{2m-2k-2}$  increases as  $y$  increases. Thus  $G_{\text{seq}}(\lambda)$  decreases as  $y$  increases. However,  $y$  decreases as  $\lambda$  increases, and this proves the fact that  $G_{\text{seq}}(\lambda)$  is a monotonically increasing function of  $\lambda$ .

For the pure-initial-state case,  $r = 1$ , and Eq. (18) gives

$$G_{\text{seq}}(\lambda) = m \frac{y - 1}{y^m - 1}, \quad (\text{A6})$$

where  $y = 1/\lambda^2$ . Then

$$y^m - 1 = (y - 1) \sum_{k=0}^{m-1} y^k \quad (\text{A7})$$

gives

$$G_{\text{seq}}(\lambda) = \frac{m}{\sum_{k=0}^{m-1} y^k}. \quad (\text{A8})$$

This is a monotonically decreasing function of  $y \geq 1$  and thus attains a maximum of 1 at  $y = 1$ . Thus  $0 \leq G_{\text{seq}}(\lambda) \leq 1$  for a pure initial state, where the lower bound stems from the fact that the gain is a ratio of positive quantities.

For the mixed-initial-state case,  $G_{\text{seq}}(\lambda)$  is a monotonically increasing function of  $\lambda$  and attains a maximum of  $m$  when  $\lambda = 1$ . This shows that  $0 \leq G_{\text{seq}}(\lambda) \leq m$  when  $r < 1$ .

#### APPENDIX B: SYMMETRIES IN THE DIAGONAL TERMS OF $\hat{\rho}_f$

Equations (25) give that the diagonal terms of  $\hat{\rho}_f$  arise only from the action of the channel on

$$\hat{\rho}_{\text{prep diag}} := \sum_{x=0}^{(N-1)/2} d_{j(x)} [|x\rangle\langle x| + |N-x\rangle\langle N-x|] \quad (\text{B1})$$

and that this will be mapped to the diagonal component of the final density operator, denoted  $\hat{\rho}_{f \text{ diag}}$  and defined via  $\hat{\rho}_{\text{prep diag}} \xrightarrow{\hat{\Gamma} \otimes \dots \otimes \hat{\Gamma}} \hat{\rho}_{f \text{ diag}}$ . A useful expression for  $\hat{\rho}_{f \text{ diag}}$  involves the following representation of the channel on any diagonal operator. Equation (25b) gives

$$|x\rangle\langle x| \xrightarrow{\hat{\Gamma}} p|x\rangle\langle x| + q\hat{\sigma}_x|x\rangle\langle x|\hat{\sigma}_x. \quad (\text{B2})$$

Thus if the channel acts on the rightmost qubit, labeled 1, then its action on the diagonal component of the density

operator is

$$\hat{\rho}_{\text{prep diag}} \xrightarrow{\hat{\Gamma}^{(1)}} p \hat{\rho}_{\text{prep diag}} + q \hat{X}_1 \hat{\rho}_{\text{prep diag}} \hat{X}_1, \quad (\text{B3})$$

where  $\hat{X}_1 := \hat{I} \otimes \cdots \otimes \hat{I} \otimes \hat{\sigma}_x$  and the superscript on  $\hat{\Gamma}$  indicates action on qubit 1. Suppose that the channel acts on qubit 1 and then on qubit 2. This maps the diagonal component of the prepared density operator as

$$\begin{aligned} \hat{\rho}_{\text{prep diag}} &\xrightarrow{\hat{\Gamma}^{(1)}} p \hat{\rho}_{\text{prep diag}} + q \hat{X}_1 \hat{\rho}_{\text{prep diag}} \hat{X}_1 \\ &\xrightarrow{\hat{\Gamma}^{(2)}} p^2 \hat{\rho}_{\text{prep diag}} \\ &\quad + pq[\hat{X}_1 \hat{\rho}_{\text{prep diag}} \hat{X}_1 + \hat{X}_2 \hat{\rho}_{\text{prep diag}} \hat{X}_2] \\ &\quad + q^2 \hat{X}_2 \hat{X}_1 \hat{\rho}_{\text{prep diag}} \hat{X}_2 \hat{X}_1, \end{aligned} \quad (\text{B4})$$

where  $\hat{X}_2 := \hat{I} \otimes \cdots \otimes \hat{I} \otimes \hat{\sigma}_x \otimes \hat{I}$ . This extends to the action of the channel once on each of qubits  $1, 2, 3, \dots, m$  and gives

$$\begin{aligned} \hat{\rho}_{\text{prep diag}} &\mapsto \hat{\rho}_{\text{f diag}} \\ &= \sum_{k=0}^m q^k p^{m-k} \\ &\quad \times \sum \hat{X}_{l_k} \cdots \hat{X}_{l_1} \hat{\rho}_{\text{prep diag}} \hat{X}_{l_k} \cdots \hat{X}_{l_1}, \end{aligned} \quad (\text{B5})$$

where the inner sum is over all  $(l_k, \dots, l_1)$  that satisfy  $l_k > l_{k-1} > \cdots > l_1$  and range over the entire possibilities starting with  $l_1 = 1$  to  $l_k = m$ . If  $k = 0$ , the inner sum is taken to mean  $\hat{\rho}_{\text{prep diag}}$ . For example, if  $k = 3$  and  $m = 4$ , there are three indices  $l_3 > l_2 > l_1$ , and the summation range yields the following possibilities for  $(l_3, l_2, l_1)$ :  $(3, 2, 1), (4, 2, 1), (4, 3, 1), (4, 3, 2)$ . This consists of the set of all flips on three out of the four qubits with the least significant label. A more symmetrical alternative is

$$\hat{\rho}_{\text{f diag}} = \sum_{k=0}^m q^k p^{m-k} \frac{1}{k!} \sum \hat{X}_{l_k} \cdots \hat{X}_{l_1} \hat{\rho}_{\text{prep diag}} \hat{X}_{l_k} \cdots \hat{X}_{l_1}, \quad (\text{B6})$$

where the sum is over all  $m \geq l_k, l_{k-1}, \dots, l_1 \geq 1$ , where no two indices are equal. We introduce the following notation to render this more compact. Let  $\vec{l} := (l_k, \dots, l_1)$ , where  $m \geq l_k, l_{k-1}, \dots, l_1 \geq 1$  and no two elements in this list are equal. Then define  $\hat{X}_{\vec{l}} := \hat{X}_{l_k} \cdots \hat{X}_{l_1}$ . It follows that

$$\hat{\rho}_{\text{f diag}} = \sum_{k=0}^m \frac{q^k p^{m-k}}{k!} \sum_{\vec{l}} \hat{X}_{\vec{l}} \hat{\rho}_{\text{prep diag}} \hat{X}_{\vec{l}}. \quad (\text{B7})$$

We use this to prove that

$$\langle N - x | \hat{\rho}_{\text{f}}(\lambda) | N - x \rangle = \langle x | \hat{\rho}_{\text{f}}(\lambda) | x \rangle. \quad (\text{B8})$$

To do so, note that  $|N - x\rangle = \hat{X}_n \cdots \hat{X}_1 |x\rangle$  and let  $\hat{X}_{\text{tot}} := \hat{X}_n \cdots \hat{X}_1$ . Thus, using  $\hat{X}_{\text{tot}}^\dagger = \hat{X}_{\text{tot}}$ ,

$$\begin{aligned} \langle N - x | \hat{\rho}_{\text{f}}(\lambda) | N - x \rangle &= \langle N - x | \hat{\rho}_{\text{f diag}} | N - x \rangle \\ &= \langle x | \hat{X}_{\text{tot}} \hat{\rho}_{\text{f diag}} \hat{X}_{\text{tot}} | x \rangle. \end{aligned} \quad (\text{B9})$$

Equation (B7) gives

$$\begin{aligned} &\langle N - x | \hat{\rho}_{\text{f}}(\lambda) | N - x \rangle \\ &= \langle x | \sum_{k=0}^m \frac{q^k p^{m-k}}{k!} \sum_{\vec{l}} \hat{X}_{\text{tot}} \hat{X}_{\vec{l}} \hat{\rho}_{\text{prep diag}} \hat{X}_{\vec{l}} \hat{X}_{\text{tot}} | x \rangle \\ &= \sum_{k=0}^m \frac{q^k p^{m-k}}{k!} \sum_{\vec{l}} \langle x | \hat{X}_{\vec{l}} \hat{X}_{\text{tot}} \hat{\rho}_{\text{prep diag}} \hat{X}_{\text{tot}} \hat{X}_{\vec{l}} | x \rangle \end{aligned} \quad (\text{B10})$$

since  $\hat{X}_{\text{tot}}$  commutes with  $\hat{X}_{\vec{l}}$ . Then Eq. (B1) gives  $\hat{X}_{\text{tot}} \hat{\rho}_{\text{prep diag}} \hat{X}_{\text{tot}} = \hat{\rho}_{\text{prep diag}}$ . This and Eq. (B10) give

$$\begin{aligned} &\langle N - x | \hat{\rho}_{\text{f}}(\lambda) | N - x \rangle \\ &= \langle x | \sum_{k=0}^m \frac{q^k p^{m-k}}{k!} \sum_{\vec{l}} \hat{X}_{\vec{l}} \hat{\rho}_{\text{prep diag}} \hat{X}_{\vec{l}} | x \rangle \\ &= \langle x | \hat{\rho}_{\text{f}}(\lambda) | x \rangle. \end{aligned} \quad (\text{B11})$$

### APPENDIX C: DIAGONAL TERMS OF $\hat{\rho}_{\text{f}}$

Let the binary representation of  $x$  be  $x = x_n \cdots x_1$ . Then  $d_{\text{f } x} = \langle x | \hat{\rho}_{\text{f}} | x \rangle$  and Eq. (B5) give

$$\begin{aligned} d_{\text{f } x} &= \sum_{k=0}^m q^k p^{m-k} \sum \langle x_n \cdots \bar{x}_{l_k} \cdots \bar{x}_{l_1} \cdots x_1 | \hat{\rho}_{\text{prep diag}} | x_n \\ &\quad \cdots \bar{x}_{l_k} \cdots \bar{x}_{l_1} \cdots x_1 \rangle, \end{aligned} \quad (\text{C1})$$

with the same constraints for the inner sum as for Eq. (B5) and where  $\bar{x}_l = 1 - x_l$ . We shall evaluate the inner sum for any value of  $k$ , which represents the number of flips on the bits within the binary representation of  $x$ .

The fact that the diagonal terms of  $\hat{\rho}_{\text{f}}$  depend only on the number of (and not their order) zeros,  $u$ , in the  $n - m$  most significant bits and also the number of zeros,  $v$ , in the  $m$  least significant bits implies that it is sufficient to consider  $d_{\text{f } x}$  where the binary representation of  $x$  is

$$x = \underbrace{0 \cdots 0}_u \underbrace{1 \cdots 1}_{n-m-u} \underbrace{1 \cdots 1}_{m-v} \underbrace{0 \cdots 0}_v. \quad (\text{C2})$$

Here Eqs. (22) and (C1) give

$$d_{\text{f } x} = \sum_{k=0}^m q^k p^{m-k} \sum d_{j(x_n \cdots \bar{x}_{l_k} \cdots \bar{x}_{l_1} \cdots x_1)} \quad (\text{C3})$$

with the same limits for the inner sum. These limits can be modified by observing that  $d_{j(x_n \cdots \bar{x}_{l_k} \cdots \bar{x}_{l_1} \cdots x_1)}$  depends only on the number of zeros and ones in the binary representation of  $x$  together with the number and arrangement of flips. Suppose that, of the  $k$  flips,  $l$  occur on the rightmost cluster of  $v$  bits. Thus  $k - l$  occur on the second from the right cluster of  $m - v$  bits. Then the bit representation,  $x_n \cdots \bar{x}_{l_k} \cdots \bar{x}_{l_1} \cdots x_1$  contains  $u$  zeros from the leftmost cluster, zero from the next cluster to the right,  $(k - l)$  from the second to the right cluster, and  $v - l$  from the rightmost cluster. Thus the total number of zeros in this bit string are  $u + v + k - 2l$ , and

$$d_{j(x_n \cdots \bar{x}_{l_k} \cdots \bar{x}_{l_1} \cdots x_1)} = d_{u+v+k-2l}. \quad (\text{C4})$$

The exact location of the flips within each cluster is irrelevant. Thus within the inner sum of Eq. (C3) there are  $\binom{v}{l} \binom{m-v}{k-l}$  ways



of attaining  $d_{u+v+k-2l}$ , consisting of  $\binom{v}{l}$  ways of flipping  $l$  bits in the rightmost cluster together with  $\binom{m-v}{k-l}$  ways of flipping  $k-l$  in the second from the right cluster. Finally, not every value of  $l$  is possible, and these are constrained by  $0 \leq l \leq v$  (at most  $v$  flips in the rightmost cluster) and  $0 \leq k-l \leq m-v$  (at most  $m-v$  flips in the second from the right cluster). Taken together, these give  $\max(0, v-m+k) \leq l \leq \min(k, v)$ .

Combining these yields Eq. (30).

#### APPENDIX D: QUANTUM FISHER INFORMATION

We shall show that

$$H_x = \frac{2}{d_{f,x}^2 - \lambda^{2m} c_{j(x)}^2} [d_{f,x} (\dot{d}_{f,x}^2 + m^2 \lambda^{2m-2} c_{j(x)}^2) - 2m \lambda^{2m-1} \dot{d}_{f,x} c_{j(x)}^2], \quad (\text{D1})$$

and the result will follow from Eq. (31). The expression for  $H_x$  comes from the eigenvalue decomposition of  $\hat{\rho}_{f,x}$ . The eigenvalues are of  $\hat{\rho}_{f,x}$ ,

$$p_{\pm} := d_{f,x} \pm \lambda^m c_{j(x)}, \quad (\text{D2})$$

and the associated eigenvectors are

$$|\phi_{\pm}\rangle := (|x\rangle \mp i|N-x\rangle)/\sqrt{2}. \quad (\text{D3})$$

The fact that the eigenvalues are independent of  $\lambda$  means that the second term on the right-hand side of Eq. (8) is zero and the first term then yields

$$H_x = \frac{1}{d_{f,x} + \lambda^m c_{j(x)}} (\dot{d}_{f,x} + m \lambda^{m-1} c_{j(x)})^2 + \frac{1}{d_{f,x} - \lambda^m c_{j(x)}} (\dot{d}_{f,x} - m \lambda^{m-1} c_{j(x)})^2. \quad (\text{D4})$$

Straightforward algebra yields the desired result.

The expression for the quantum Fisher information can be rewritten as a sum over  $u$  and  $v$ . The only relevance that each value of  $x$  has for the summand is that it determines  $u, v$ , and  $j(x) = u + v$ . Typically, many values of  $x$  will yield the same combination of values of  $u$  and  $v$ . To account for this, note that the sum in Eq. (32) runs from  $x = 00 \dots 0$  to  $x = 01 \dots 1$  (in binary notation). The fact that the leftmost bit is always zero gives two distinct cases.

In the first, where  $m < n$ , this bit structure reveals that  $1 \leq u \leq n-m$  and  $0 \leq v \leq m$ . For any choice of  $u$ , there are  $\binom{n-m-1}{u-1}$  ways in which the zeros can appear in the leftmost  $n-m$  bits, given that the leftmost single bit must be zero. There are independently  $\binom{m}{v}$  ways in which the zeros can appear in the rightmost  $m$  bits. Thus there are  $\binom{n-m-1}{u-1} \binom{m}{v}$  values of  $x$  in the range of the sum which result in exactly the same pair of values  $u$  and  $v$ . For each the contribution of the summand is identical. This means that the terms within the summand can be expressed in terms of  $u$  and  $v$  (rather than  $x$ ) and the result sum reduces to that of Eq. (33).

In the second, where  $m = n$ , clearly,  $u = 0$  and  $1 \leq v \leq n-1$ . A similar counting argument reveals that there are  $\binom{v-1}{n-1}$  ways in which the zeros can appear in the rightmost  $n-1$  bits since the rightmost bit must be zero. A similar argument then results in Eq. (34).

#### APPENDIX E: LOW-POLARIZATION CORRELATED-STATE-PROTOCOL QUANTUM FISHER INFORMATION

The correlated-state-protocol quantum Fisher information, Eqs. (33) and (34), requires  $c_j$  and  $d_f(u, v)$ , which in turn require  $d_j$ . Equations (23) and (24) yield, to second order in  $r$ ,

$$c_j \approx \frac{(2j-n)}{2^n} r, \quad (\text{E1})$$

$$d_j \approx \frac{1}{2^n} + \frac{r^2[(2j-n)^2 - n]}{2^{n+1}}. \quad (\text{E2})$$

The latter of these gives

$$d_f(u, v) = \alpha + \beta r^2, \quad (\text{E3})$$

where

$$\alpha := \sum_{k=0}^m q^k p^{m-k} \sum_{l=l_{\min}}^{l_{\max}} \binom{v}{l} \binom{m-v}{k-l} \frac{1}{2^n} \quad (\text{E4})$$

and

$$\beta := \sum_{k=0}^m q^k p^{m-k} \sum_{l=l_{\min}}^{l_{\max}} \binom{v}{l} \binom{m-v}{k-l} \times \frac{[(2u+2v+2k-4l-n)^2 - n]}{2^{n+1}}. \quad (\text{E5})$$

Both  $\alpha$  and  $\beta$  are independent of  $r$ . Then

$$\alpha = \frac{1}{2^n}, \quad (\text{E6})$$

which can be demonstrated indirectly by noting that, when  $r = 0$ , each diagonal term of the final density operator equals  $\alpha$ . However, when  $r = 0$ ,  $\hat{\rho}_0 = \hat{I}/2$ , and thus  $\hat{\rho}_i = \hat{I}/2^n$ . The channel does not alter this, and thus, when  $r = 0$ ,  $\hat{\rho}_f = \hat{I}/2^n$ . It follows that  $\alpha = 1/2^n$ . This fact can independently be verified by explicitly evaluating the three summations in  $\alpha$ .

Note that these imply

$$\dot{d}_f^2 \approx \frac{\partial \beta}{\partial \lambda} r^2. \quad (\text{E7})$$

Then Eqs. (E1), (E3), and (E6) yield that for the terms in Eqs. (33) and (34)

$$\begin{aligned} d_f^2 - \lambda^{2m} c_{u+v}^2 &\approx \frac{1}{2^{2n}}, \\ d_f (\dot{d}_f^2 + m^2 \lambda^{2m-2} c_{u+v}^2) &\approx d_f m^2 \lambda^{2m-2} c_{u+v}^2 \\ &= \frac{m^2 \lambda^{2m-2}}{2^{3n}} (2u+2v-n) r^2, \\ \dot{d}_f^2 c_{u+v} &\approx \left( \frac{\partial \beta}{\partial \lambda} \frac{2(2u+2v-n)}{2^{n+1}} \right)^2 r^6. \end{aligned}$$

Thus, if  $m < n$ , Eqs. (33) becomes

$$\begin{aligned} H_{\text{corr}}(\lambda) &\approx \sum_{v=0}^m \sum_{u=1}^{n-m} \binom{n-m-1}{u-1} \binom{m}{v} 2^{2n+1} \frac{m^2 \lambda^{2m-2}}{2^{3n}} (2u + 2v - n) r^2 \\ &= r^2 \frac{m^2 \lambda^{2m-2}}{2^{n-1}} \sum_{u=1}^{n-m} \binom{n-m-1}{u-1} \sum_{v=0}^m \binom{m}{v} (2u + 2v - n). \end{aligned} \quad (\text{E8})$$

The two summations in Eq (E8) give  $n2^{n-1}$ , and this yields the result of Eq. (39). A similar derivation gives the same result when  $m = n$ .

- 
- [1] C. M. Caves, K. S. Thorne, R. W. P. Drever, V. D. Sandberg, and M. Zimmermann, *Rev. Mod. Phys.* **52**, 341 (1980).  
[2] C. M. Caves, *Phys. Rev. D* **23**, 1693 (1981).  
[3] J. H. Shapiro and S. R. Shepard, *Phys. Rev. A* **43**, 3795 (1991).  
[4] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).  
[5] S. L. Braunstein and C. M. Caves, *Phys. Rev. Lett.* **72**, 3439 (1994).  
[6] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, *Phys. Rev. Lett.* **79**, 3865 (1997).  
[7] M. Sarovar and G. J. Milburn, *J. Phys. A* **39**, 8487 (2006).  
[8] V. Giovannetti, S. Lloyd, and L. Maccone, *Phys. Rev. Lett.* **96**, 010401 (2006).  
[9] M. Paris, *Int. J. Quantum Inf.* **7**, 125 (2009).  
[10] P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, 2010).  
[11] V. Giovannetti, S. Lloyd, and L. Maccone, *Nat. Photon.* **5**, 222 (2011).  
[12] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).  
[13] C. Adami and N. J. Cerf, *Phys. Rev. A* **56**, 3470 (1997).  
[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).  
[15] C. Cafaro and S. Mancini, *Phys. Rev. A* **82**, 012306 (2010).  
[16] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne, *Phys. Rev. Lett.* **86**, 5811 (2001).  
[17] C. A. Ryan, M. Laforest, and R. Laflamme, *New J. Phys.* **11**, 013034 (2009).  
[18] K. Banaszek, A. Dragan, W. Wasilewski, and C. Radzewicz, *Phys. Rev. Lett.* **92**, 257901 (2004).  
[19] J. C. do Nascimento and R. V. Ramos, *Microwave Opt. Technol. Lett.* **47**, 497 (2005).  
[20] M. Karpiński, C. Radzewicz, and K. Banaszek, *J. Opt. Soc. Am. B* **25**, 668 (2008).  
[21] M. Zwiernik, C. A. Pérez-Delgado, and P. Kok, *Phys. Rev. Lett.* **105**, 180402 (2010).  
[22] M. Zwiernik, C. A. Pérez-Delgado, and P. Kok, *Phys. Rev. A* **85**, 042112 (2012).  
[23] A. Fujiwara, *Phys. Rev. A* **63**, 042304 (2001).  
[24] M. Sasaki, M. Ban, and S. M. Barnett, *Phys. Rev. A* **66**, 022308 (2002).  
[25] A. Fujiwara and H. Imai, *J. Phys. A* **36**, 8093 (2003).  
[26] M. Frey, D. Collins, and K. Gerlach, *J. Phys. A* **44**, 205306 (2011).  
[27] K. Modi, H. Cable, M. Williamson, and V. Vedral, *Phys. Rev. X* **1**, 021022 (2011).  
[28] D. Collins, *Phys. Rev. A* **87**, 032301 (2013).  
[29] G. M. D'Ariano, C. Macchiavello, and P. Perinotti, *Phys. Rev. A* **72**, 042327 (2005).  
[30] S. Boixo and A. Monras, *Phys. Rev. Lett.* **100**, 100503 (2008).  
[31] D. Braun, *Eur. Phys. J. D* **59**, 521 (2010).  
[32] A. Datta, L. Zhang, N. Thomas-Peter, U. Dorner, B. J. Smith, and I. A. Walmsley, *Phys. Rev. A* **83**, 063836 (2011).  
[33] O. Pinel, P. Jian, N. Treps, C. Fabre, and D. Braun, *Phys. Rev. A* **88**, 040102 (2013).  
[34] H. Cramér, *Mathematical Methods of Statistics* (Princeton University Press, Princeton, NJ, 1946).  
[35] C. J. O'Loan, [arXiv:1001.3971](https://arxiv.org/abs/1001.3971).  
[36] Y. Watanabe, in *Formulation of Uncertainty Relation between Error and Disturbance in Quantum Measurement by Using Quantum Estimation Theory*, Springer Theses (Springer Japan, Tokyo, 2014), pp. 37–44.  
[37] O. E. Barndorff-Nielsen and R. D. Gill, *J. Phys. A* **33**, 4481 (2000).  
[38] M. A. Ballester, *Phys. Rev. A* **69**, 022303 (2004).  
[39] A. Fujiwara, *Phys. Rev. A* **70**, 012317 (2004).  
[40] M. Hotta, T. Karasawa, and M. Ozawa, *Phys. Rev. A* **72**, 052334 (2005).  
[41] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, *IEEE Trans. Inf. Theory* **54**, 5172 (2008).  
[42] B. M. Escher, R. L. de Matos Filho, and L. Davidovich, *Nat. Phys.* **7**, 406 (2011).  
[43] W. van Dam, G. M. D'Ariano, A. Ekert, C. Macchiavello, and M. Mosca, *Phys. Rev. Lett.* **98**, 090501 (2007).  
[44] A. Peres, *Phys. Rev. Lett.* **77**, 1413 (1996).  
[45] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).  
[46] H. Ollivier and W. H. Zurek, *Phys. Rev. Lett.* **88**, 017901 (2001).  
[47] S. Luo, *Phys. Rev. A* **77**, 042303 (2008).  
[48] Q. Chen, C. Zhang, S. Yu, X. X. Yi, and C. H. Oh, *Phys. Rev. A* **84**, 042313 (2011).